

UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

In the Matter of the Search of
 (Briefly describe the property to be searched
 or identify the person by name and address)

[REDACTED], Cudahy, Wisconsin

Case
 No.22-969M(NJ)

CLERK'S OFFICE

A TRUE COPY

Aug 19, 2022

s/ Laura Cronin

Deputy Clerk, U.S. District Court
 Eastern District of Wisconsin

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure of the following person or property located in the Eastern District of Wisconsin
 (identify the person or describe the property to be searched and give its location):

See Attachment A

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal (identify the person or describe the property to be seized):

See Attachment B

YOU ARE COMMANDED to execute this warrant on or before September 3, 2022 (not to exceed 14 days)

☒ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Hon. Nancy Joseph

(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box)

☐ for days (not to exceed 30) ☐ until, the facts justifying, the later specific date of

Date and time issued: 8/19/2022 @ 10:35 a.m.

Nancy Joseph
 Judge's signature

City and state: Milwaukee, WI

U.S. Magistrate Judge Nancy Joseph

Printed name and title

Return		
Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:
Inventory made in the presence of :		
Inventory of the property taken and name(s) of any person(s) seized:		
Certification		
<p>I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.</p> <div style="display: flex; justify-content: space-between;"> <div style="width: 30%;"> <p>Date: _____</p> </div> <div style="width: 65%;"> <p style="text-align: center;">_____</p> <p style="text-align: center;"><i>Executing officer's signature</i></p> <p style="text-align: center;">_____</p> <p style="text-align: center;"><i>Printed name and title</i></p> </div> </div>		

ATTACHMENT A

Property to Be Searched

The property to be searched is [REDACTED], CUDAHY, WI 53110, further described as slightly elevated two-story white house with a front porch with a north-facing door and a garage in the back.

google.com/maps/

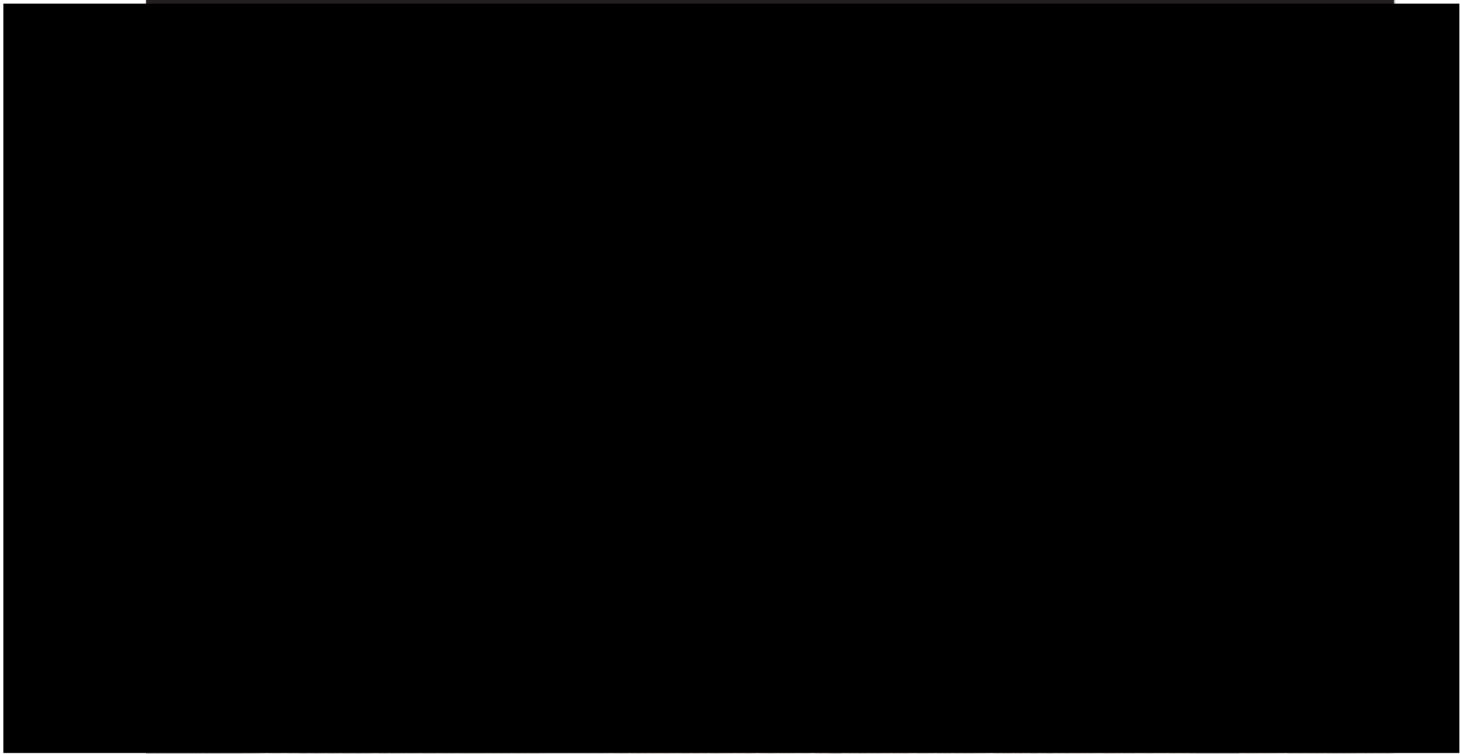
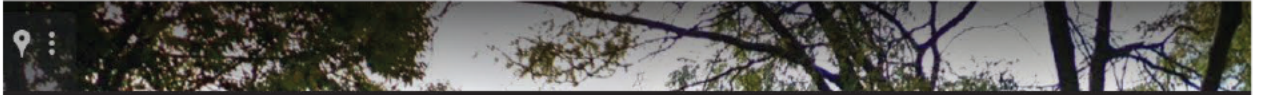


Image capture: Oct 2017 © 2022 Google

ATTACHMENT B

Property to Be Seized

1. All records relating to violations of 18 U.S.C. §§ 1028(a)(7) (possession of means of identification in connection with another federal felony offense, including wire fraud); 1029(a)(2) (use and trafficking of access devices), 1029(a)(3) (possession of 15 or more access devices); 1030(a)(2) (illegally accessing a protected computer); 1030(a)(5) (illegally damaging a protected computer); and 371 (conspiracy) (collectively, the “Subject Offenses”) involving [REDACTED] or Web Market A operators and occurring after August 26, 2020, including:

- a. Records and information relating to Web Market A;
- b. Records and information relating to an access, use, possession, or control over stolen personal information, financial information, and/or electronic devices;
- c. Records and information relating to IP address 76.215.26.107;
- d. Records and information relating to the identity or location of the suspect(s);
- e. Records and information relating to malicious software;
- f. Records and information relating to finances, including financial institutions, financial instruments;
- g. Records and information relating to virtual currency such as bitcoin.

2. Computers or storage media used as a means to commit the violations described above.

3. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, “COMPUTER”):

- a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, “chat,” instant messaging logs, photographs, and correspondence;
- b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- c. evidence of the lack of such malicious software;
- d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;
- e. evidence indicating the computer user’s state of mind as it relates to the crime under investigation;
- f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
- g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
- h. evidence of the times the COMPUTER was used;
- i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

- j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
 - k. records of or information about Internet Protocol addresses used by the COMPUTER;
 - l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;
 - m. contextual information necessary to understand the evidence described in this attachment.
4. Routers, modems, and network equipment used to connect computers to the Internet.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term “storage medium” includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

During the execution of the search of the property described in Attachment A, law enforcement personnel are authorized to (1) press or swipe the fingers (including thumbs) of [REDACTED] to the fingerprint scanner of the device(s); (2) hold the device(s) in front of the face of [REDACTED] and activate the facial recognition feature; and/or (3) hold the device(s) in front of the face of [REDACTED] and activate the iris recognition feature, for the purpose of attempting to unlock the device(s) in order to search the contents as authorized by this warrant.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

UNITED STATES DISTRICT COURT

for the
Eastern District of Wisconsin

CLERK'S OFFICE

A TRUE COPY

Aug 19, 2022

s/ Laura Cronin

Deputy Clerk, U.S. District Court
Eastern District of WisconsinIn the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

[REDACTED], Cudahy, Wisconsin.

Case No. 22-969M(NJ)

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A

located in the Eastern District of Wisconsin, there is now concealed (identify the person or describe the property to be seized):

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 USC 371, 1028(a)(7)	Conspiracy, Identity Theft
18 USC 1029(a)(2), (a)(3)	Access Device Fraud
18 USC 1030(a)(2), (a)(5).	Computer Fraud and Abuse

The application is based on these facts:

See attached affidavit

☒ Continued on the attached sheet.☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the att

Applicant's signature

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by
_____ telephone _____ (specify reliable electronic means).

Date: 8/19/2022

Judge's signature

City and state: Milwaukee, WI

U.S. Magistrate Judge Nancy Joseph

Printed name and title

**AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER
RULE 41 FOR A WARRANT TO SEARCH AND SEIZE**

I, [REDACTED], being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises known as [REDACTED], Cudahy, WI 53110, hereinafter "PREMISES," further described in Attachment A, for the things described in Attachment B.

2. I am a Special Agent with the FBI and have been a Special Agent since [REDACTED]

[REDACTED]
[REDACTED]
[REDACTED] I am currently assigned to the FBI Milwaukee Division's Cyber Crime Task Force. As a Special Agent for the FBI, I investigate criminal computer intrusion matters involving botnets, distributed denial of service attacks, the distribution of spam, the use of malware, identity theft, and other computer-based fraud.

3. This affidavit is based upon information supplied to me by other law enforcement officers, including other Special Agents employed by the FBI. It is also based upon my personal involvement in this investigation and on my training and experience. In submitting this affidavit, I have not included every fact known to me about the investigation, but instead have included only those facts that I believe are sufficient to establish probable cause to support this seizure warrant application.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. §§ 1028(a)(7) (possession of means of identification in connection with another federal felony offense, including wire fraud); 1029(a)(2) (use and trafficking of access devices); 1029(a)(3) (possession of 15 or more access devices); 1030(a)(2) (illegally accessing a protected computer); 1030(a)(5) (illegally damaging a protected computer); and 371 (conspiracy) (collectively, the “Subject Offenses”), have been committed by individuals (both known and unknown to law enforcement) associated with the operation of Genesis Market, as well as by [REDACTED], who resides at the PREMISES.

PROBABLE CAUSE

Background Regarding the Genesis Market Investigation

5. Since [REDACTED], the FBI has been investigating an illicit online marketplace named Genesis Market.¹ Genesis Market is primarily hosted at the Internet domain “genesis.market.”² Genesis Market’s operators compile stolen data (e.g., computer and mobile

¹ In Attachment B, Genesis Market is referred to “Web Market A.” At this time, Genesis Market remains active and disclosure of the name of the market would potentially alert its operators of law enforcement action being taken against the users and operators. This may prompt users of the market to notify others of law enforcement action, flee, and/or destroy evidence. Accordingly, the government will file a separate motion to seal the warrant affidavit.

² A domain name is a way to identify computers on the Internet, using a series of characters that correspond with a particular IP address. Genesis Market is also associated with certain backup domains in case the primary domain is shut down or taken offline for any reason. Those backup domains include the website “g3n3sis.org,” as well as the TOR domain “genesiswiwn7p7lmbvimup7v767e64rcw6o3kfcnobu3nxisteprx2qd.onion.” TOR is short for “The Onion Router” and is free, publicly available software for enabling anonymous communication over the internet. The TOR software is designed to enhance users’ privacy online by bouncing their communications around a

device identifiers, email addresses, usernames, and passwords) from malware-infected³ computers around the globe and package it for sale on the market.⁴ Genesis Market has been the subject of various cybersecurity presentations and news stories. For example, CBS News ran a story on Genesis Market in September 2021.⁵

6. The packages advertised for sale on Genesis Market vary by price and many packages are available for around \$10 to \$20 per package. The price appears to vary based on three primary factors: (1) the number of online accounts (“resources”) associated with the package (*e.g.*, accounts with legitimate credentials for platforms like Amazon, Netflix, Gmail, etc., are more valuable); (2) how recently the package was compromised with malware; and (3) whether there is a “fingerprint” associated with the package. A fingerprint is a group of identifiers that third-party applications or websites use to identify a computer or device. These fingerprints allow the applications or websites to confirm that the device is a trusted source. In

distributed network of relay computers run by volunteers around the world, thereby masking the user's actual IP address, which could otherwise be used to identify a user.

³ Malware, or malicious software, refers to any piece of software that is written to damage and/or steal data from an Internet connected device. Viruses, trojans, spyware, and ransomware are all different types of malware.

⁴ Genesis Market refers to these packages of stolen data as “bots” on their site; however, typically, an Internet bot refers to a piece of software that runs automated tasks over the Internet. Since Genesis Market’s use of the word “bot” strays from the normal meaning, the term “package” is used throughout this request.

⁵ See Dan Patterson, *Inside Genesis: The market created by cybercriminals to make millions selling your digital identity*, September 9, 2021, available at <https://www.cbsnews.com/news/genesis-cybercriminal-market-ransomware/> (last visited August 5, 2022).

situations where a fingerprint is associated with a package, Genesis Market provides the purchaser with a proprietary plugin (*i.e.*, an Internet browser extension that provides additional functionality). This proprietary plugin amplifies that purchaser's ability to control and access the package's data and masquerade as the victim device.

7. Genesis Market's operators have advertised Genesis Market on prominent online criminal forums, including exploit.in and xss.is. Those advertisements include news, updates, and information regarding Genesis Market. For example, the advertisements have included (1) information about packages for sale on Genesis Market; (2) specific replies to users requesting packages located in specific countries; and (3) updates regarding the tools available through Genesis Market.

8. Genesis Market users can gain initial access to Genesis Market via an invitation from a Genesis Market operator on a cybercriminal forum, or via an invitation from an individual who already has an account on Genesis Market. The invitations are for one-time use and in the form of an alphanumeric text string. Once a prospective new user receives an invitation, the new user can go to a Genesis Market domain to create a username and password. Genesis Market then requests the new user to associate their Jabber ID⁶ or email address with that new account. Analysis by law enforcement has found that a Jabber ID or email address is not absolutely

⁶ Jabber is a chat and communications platform akin to AOL Instant Messenger. It is prominent among cybercriminal operators because it is considered exceptionally secure.

required when registering an account, nor is the Jabber ID or email address verified by Genesis Market administrators. Nonetheless, the vast majority of Genesis users have registered with a Jabber ID or email address, as it is one of the fields to enter registration data when creating a new account.

9. While conducting covert operations, law enforcement has observed that for new users logged into Genesis Market, the front page generally displays a “dashboard” of information, including the number of packages listed for sale and a “Genesis Wiki” page that walks a new user through Genesis Market’s platform and how to use it. Below is a screenshot taken April 1, 2021, of the front page of Genesis Market.⁷ The front page displays the total amount of “bots” (packages) available for sale on Genesis Market at that time, categorized by country. This page appears immediately after the user logs into his or her account. The tabs on the left allow for the Genesis Market user to traverse the market:

⁷ Portions of the screenshots in this affidavit have been redacted or omitted to conceal information that might identify accounts used covertly by investigators.

genesis

Dashboard Home

Genesis Wiki

News

Bots 350k+

Generate FP

Orders

Purchases 8 91

Payments 8

Tickets 1

Software 6.3 (19.0)

Profile

Invites

Logout

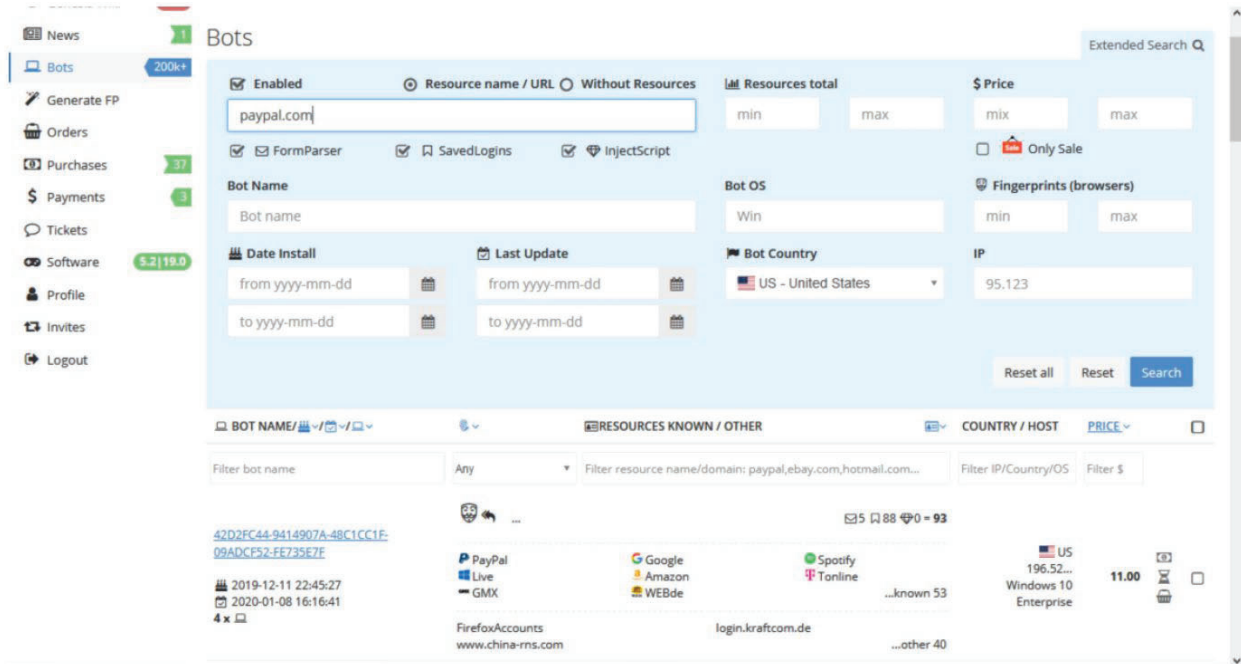
Have insider info about Genesis.market related investigation? Write us, we are interested.

Available Bots

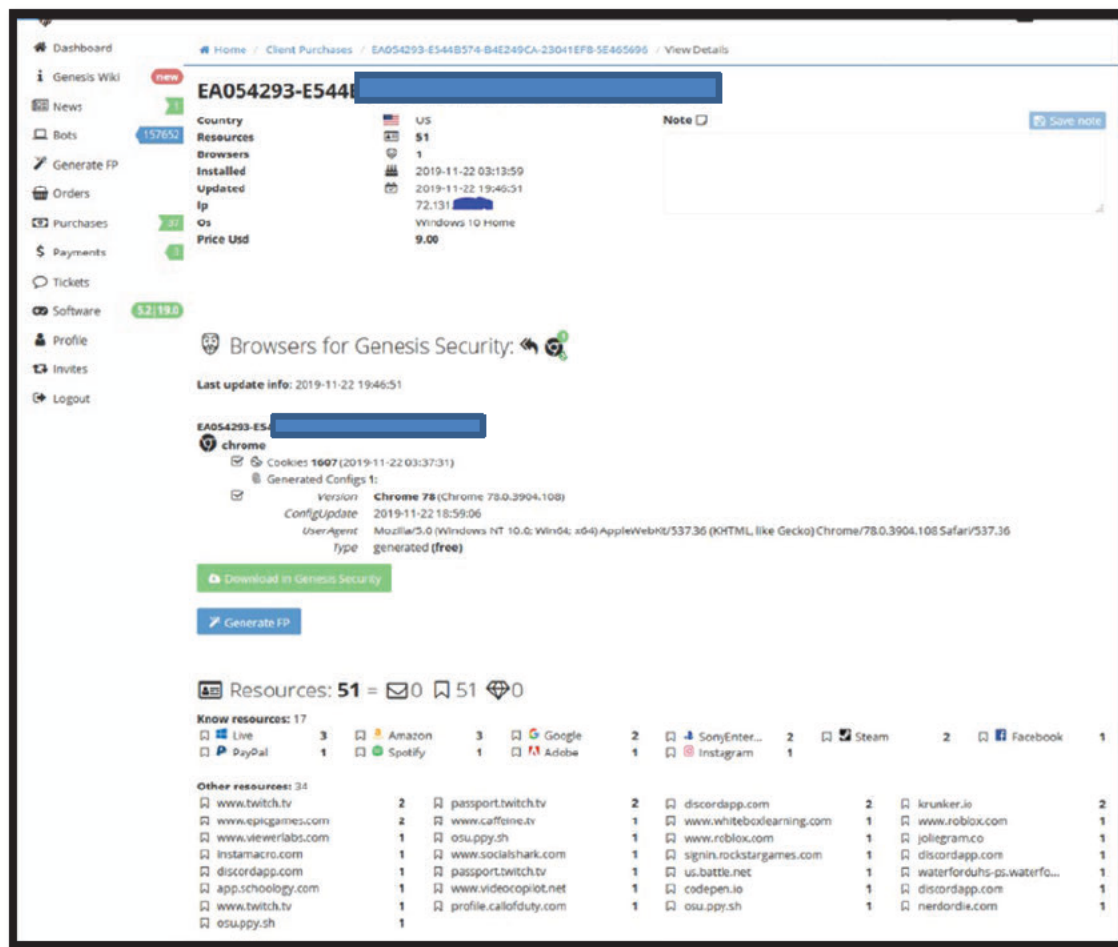
COUNTRY	LAST 24H	LAST WEEK	LAST MONTH	AVAILABLE
Overall				
218	+22	+4210	+25476	377326
Grouped by				
US	+3	+477	+3388	13625
IT	+2	+557	+2878	51196
FR	+3	+345	+2018	21074
ES	+1	+314	+1931	31370
PL	+1	+305	+1826	14694
AR	+1	+256	+1795	11532
RO	+4	+320	+1648	11309
PT		+177	+1154	21928
CL		+180	+1141	4050
HU		+156	+943	9353
GR		+148	+793	5969
NP		+91	+676	5553
NL	+1	+115	+668	7537
CA		+92	+640	2688
BG	+1	+87	+539	4473
BE		+96	+465	6837
SK		+59	+375	2822
AU		+48	+364	3127
SE	+2	+56	+363	4971
HR		+74	+340	2558
GE		+58	+320	1337
more 198				

10. Genesis Market also features a search function that allows a user to search for packages based on areas of interest (e.g., banking information, social media accounts, etc.), country of origin, price, and the date of infection (i.e., the date the victim device was infected

with malware). Below is a screenshot taken on November 13, 2020, showing the search function on Genesis Market:
























11. When a user purchases a package, the user receives access to all the identifiers associated with the package, including, but not necessarily limited to, device information, such as operating system, IP address, keyboard language, and time zone information, as well as access credentials, such as usernames and passwords, for compromised accounts. Below is a screenshot taken on November 22, 2019, of an FBI Online Covert Employee's purchase of a Genesis Market package:



12. Below is a screenshot dated November 22, 2019, relating to the same victim package as above, showing the email addresses and passwords (both of which are redacted for the purposes of this affidavit) that are provided to the purchaser of the victim package:

Last update Saved Logins: 2019-11-22 08:55:29
 Last update Form Parser: 1970-01-01 00:00:00
 Last update Inject Script: 1970-01-01 00:00:00

RESOURCE NAME / URL / LOGIN / PASSWORD / ...	SOURCE	DATASETS	BROWSER	KNOWN	GRABBED / UPDATED
	Any	Any	Any	Any	
 https://www.viewerlabs.com/register "Login": [REDACTED]@gmail.com "Password": [REDACTED]	 Saved Logins	LoginData	 chrome	no	2019-11-22 03:13:59 2019-11-22 08:55:29
EA054293-E544B574-B4E249CA-23041EF8-5E465696					
 https://account.sonyentertainmentnetwork.com/	 Saved Logins	LoginData	 chrome	yes	2019-11-22 03:13:59 2019-11-22 08:55:29
EA054293-E544B574-B4E249CA-23041EF8-5E465696					
 https://www.whiteboxlearning.com/login	 Saved Logins	LoginData	 chrome	no	2019-11-22 03:13:59 2019-11-22 08:55:29
EA054293-E544B574-B4E249CA-23041EF8-5E465696					
 https://www.amazon.com/ap/signin	 Saved Logins	LoginData	 chrome	yes	2019-11-22 03:13:59 2019-11-22 08:55:29
EA054293-E544B574-B4E249CA-23041EF8-5E465696					
 https://www.roblox.com/	 Saved Logins	LoginData	 chrome	no	2019-11-22 03:13:59 2019-11-22 08:55:29
EA054293-E544B574-B4E249CA-23041EF8-5E465696					
 https://accounts.google.com/signin/v2/si...	 Saved Logins	LoginData	 chrome	yes	2019-11-22 03:13:59 2019-11-22 08:55:29
EA054293-E544B574-B4E249CA-23041EF8-5E465696					
 https://login.live.com/ppsecure/post.srf	 Saved Logins	LoginData	 chrome	yes	2019-11-22 03:13:59 2019-11-22 08:55:29

13. When users have questions or issues with Genesis Market, they can submit “tickets” via a “Ticket” tab on the Genesis Market website, which enables them to communicate with Genesis Market operators.

14. Purchases made through Genesis Market are conducted using virtual currency, such as bitcoin.⁸ Before a purchase can be made, however, the user must first deposit a sum of virtual currency into their Genesis Market account. This is done through the “Payments” tab on the Genesis Market website, wherein the user can choose the type of virtual currency they want to use. If the user chose bitcoin, for example, the user would then (1) enter the amount in U.S. dollars that they want credited to their account, (2) receive a one-time-use bitcoin address, along with the converted bitcoin amount, and then (3) they would use that bitcoin address to send bitcoin to Genesis Market.⁹ Once the user sends the bitcoin to the one-time-use address, the user is prompted to wait several minutes for the transaction to complete, and then the user will ultimately see that their Genesis Market account is credited with the requested amount. Once the account is credited, the user can purchase packages from Genesis Market.

15. As of August 8, 2022, there were approximately 441,299 packages listed for sale on Genesis Market. Each package represents a single, compromised computer or device.

⁸ Virtual currencies, such as bitcoin, are digital tokens of value circulated over the Internet as substitutes for traditional fiat currency. Virtual currencies are not issued by any government or bank like traditional fiat currencies such as the U.S. dollar, but rather are generated and controlled through computer software. Bitcoin is currently the most well-known virtual currency in use. Investigators found that Genesis Market also accepted Litecoin (an alternative to bitcoin), and in 2022 started accepting Monero (an anonymity enhanced virtual currency).

⁹ Over the course of the investigation, investigators found that Genesis Market utilized a third-party service, [REDACTED] to process the virtual currency transactions.

According to Genesis Market's website, the packages are located across North America (including throughout the United States), Europe, South America, and parts of Asia.

16. As part of the investigation, the FBI has covertly operated several Genesis Market accounts and has funded the purchase of approximately 115 packages through Genesis Market. Through these accounts, the FBI has monitored activity on Genesis Market and interacted with Genesis Market operators through the "Ticket" function. The FBI has reviewed the data from purchased packages and determined that Genesis Market is, in fact, collecting and selling victims' personal identifying information that has been stolen from devices located around the world. For instance, FBI agents identified seven packages that consisted of data taken from devices of victims located in Wisconsin. FBI agents showed seven victim device owners the usernames and passwords that the agents had obtained via Genesis Market, and the victims confirmed that the usernames and passwords belonged to them and had been stolen.

17. In December 2020, law enforcement, via mutual legal assistance request and in coordination with authorities in another country, obtained a forensic image of a server that contained the Genesis Market database (referred to herein as "Database A"). The database included, among other things, Genesis Market's administrator logs; user logs; lists of all packages sold on the marketplace; payment transaction logs; malware used by Genesis Market administrators; and other pieces of information related to the market.

18. The data included information from more than 33,000 Genesis Market user accounts, including usernames and email addresses; IP address history; search history; virtual

currency transactions; the number of packages purchased by the user; and the data contained within the packages purchased by the user.

19. After law enforcement obtained a copy of the Genesis Market Database A server, the Genesis Market operators removed their website from that server and utilized hosting infrastructure from other companies in other countries.

20. Then, in May 2022, law enforcement, via mutual legal assistance request and in coordination with authorities in another country, obtained a forensic image of a server that contained the Genesis Market database (referred to herein as “Database B”). The database included the same types of information described above, including information from more than 55,000 Genesis Market user accounts.

Genesis Market User ID 26936

21. According to data obtained from the Database A server, Genesis Market User ID 26936, with username [REDACTED] (hereinafter “User 26936”), engaged in the following relevant activity on Genesis Market:

- a. User 26936’s Genesis Market account was created on or around August 26, 2020.
- b. Between approximately August 26, 2020, through December 4, 2020, User 26936 logged into Genesis Market almost exclusively from IP Address 76.215.26.107. Specifically, between August 30, 2020, and December 4, 2020, User 26936 logged into Genesis Market approximately 59 times.

- c. During that time, User 26936 purchased two packages on Genesis Market. These two packages together contained approximately 281 usernames and passwords for various stolen accounts, including Apple, Amazon, PayPal, and other social media, communication, banking, and video game accounts.
- d. On August 26, 2020, and August 28, 2020, User 26936 conducted two virtual currency deposits into Genesis Market. These deposits were made through an account at a U.S.-based virtual currency exchange (“VCE 1”).

Identification of Genesis User ID 26936

22. As discussed below, evidence indicates that User 26936 is [REDACTED] whose date of birth is [REDACTED]. Physical surveillance, Wisconsin Department of Transportation records, and open-source database searches indicate that [REDACTED] resides at the PREMISES with [REDACTED], date of birth [REDACTED], and [REDACTED], date of birth [REDACTED].

23. Over the course of the investigation, law enforcement determined that, during the time User 26936 was logging into Genesis Market via IP Address 76.215.26.107, IP Address 76.215.26.107 was owned by AT&T. In response to legal process, AT&T provided information

[REDACTED]

showing that, from approximately May 22, 2020, through July 27, 2021, IP Address 76.215.26.107 was registered to AT&T customer [REDACTED], with a billing address listed as [REDACTED], Cudahy, WI, 53110 (the PREMISES).

24. Further, in response to legal process, VCE 1 provided information associated with the virtual currency transactions conducted by User 26936 to fund User 26939's Genesis Market account. The information from VCE 1 showed that the VCE 1 account associated with the transaction was registered to [REDACTED] of [REDACTED], Cudahy, WI 53110 (the PREMISES). The email address associated with that VCE 1 account was [REDACTED].¹¹

As required by the Bank Secrecy Act, VCE 1 collects know-your-customer (KYC) information about its users. The KYC information associated with [REDACTED] VCE 1 account included images of [REDACTED] driver's license and [REDACTED] driver's license. Both licenses listed the driver's address as the PREMISES.¹² That said, as discussed below evidence collected thus far indicates that [REDACTED] was the actual user of the VCE 1 account.

¹¹ Portions of the email addresses and passwords referenced in this affidavit have been redacted or modified with "X's" for privacy protection purposes; however, I have left the portions of the identifiers that indicate they are used by [REDACTED]

¹² Information from VCE 1 showed that [REDACTED] driver's license was used to attempt to verify the account; however, VCE 1 could not authenticate the license with other data associated with the VCE 1 account registration. Thus, while [REDACTED] information was listed in the account, VCE 1 listed the license as "failing" authentication.

25. Additionally, information from VCE 1 showed that the VCE 1 account was regularly accessed by IP Address 76.215.26.107. Importantly, as described above, User 26936's Genesis Market account was also accessed regularly via IP Address 76.215.26.107. Further, the VCE 1 data showed that the VCE 1 account was funded by a PayPal account associated with email address [REDACTED] as well as by Visa debit cards under the name [REDACTED]. The VCE 1 data also showed activity from the VCE 1 account to the bitcoin addresses used by Genesis Market.

26. A review of the VCE 1 data also showed that the VCE 1 account was accessed via at least three devices from approximately June 19, 2020 through July 22, 2022. The data identified the devices as an iPhone, a Macintosh device, and a device using a Windows operating system.

27. On July 21, 2022, FBI conducted surveillance at the PREMISES. At about 7:10 a.m. CDT, an individual who appeared to be [REDACTED] exited the PREMISES with a duffel bag, and entered the driver's seat of a black Toyota Corolla, bearing license plate [REDACTED] and drove away from the PREMISES. Records from the State of Wisconsin show that the vehicle was registered to [REDACTED].

28. Finally, data collected from the Database B server (as described above in Paragraph 20) indicated that User 26396 was active as of August 27, 2021, and last utilized IP Address 76.215.26.107 to access Genesis Market on May 30, 2021. Further, the data from the Database A server and the Database B server showed that the password for the account was

[REDACTED] and that User 26396 used the Genesis Market search function to search for, among other things, “Cash-App,” PayPal,” “Coinbase,” and “Venmo,” which, based on my review of Genesis Market data, indicates that User 26396 was interested in searching Genesis Market for packages that had stolen credentials for those financial service providers.

29. As of August 8, 2022, FBI surveillance showed that [REDACTED], [REDACTED]

[REDACTED], [REDACTED], and an unidentified female child, [REDACTED]
[REDACTED], continued to reside at the PREMISES.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

30. As described above and in Attachment B, this application seeks permission to search for records that might be found on the PREMISES, in whatever form they are found. One form in which the records might be found is data stored on a computer’s hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

31. *Probable cause.* I submit that if a computer or storage medium is found on the PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet.

Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

32. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the PREMISES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the

sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (*e.g.*, registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculcating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the

computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (*e.g.*, a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (*e.g.*, internet searches indicating criminal planning), or consciousness of guilt (*e.g.*, running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

- c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.
- f. I know that when an individual uses a computer to obtain unauthorized access to a victim computer over the Internet, the individual's computer will

generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

33. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

- a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing

34. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

35. Because several people share the PREMISES as a residence, it is possible that the PREMISES will contain storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that that it is possible that the things described in this warrant could be found on any of those computers or storage media, the warrant applied for would permit the seizure and review of those items as well.

UNLOCKING ELECTRONIC DEVICES USING BIOMETRIC FEATURES

36. The warrant I am applying for would permit law enforcement to obtain from certain individuals the display of physical biometric characteristics (such as fingerprint, thumbprint, or facial characteristics) in order to unlock devices subject to search and seizure pursuant to this warrant. I seek this authority based on the following:

a. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the

ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners and facial recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

b. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called “Touch ID,” which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device’s Touch ID sensor, which is found in the round button (often referred to as the “home” button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

c. If a device is equipped with a facial recognition feature, a user may enable the ability to unlock the device through his or her face. For example, Apple offers a facial recognition feature called “Face ID.” During the Face ID registration process, the user holds the device in front of his or her face. The device’s camera then analyzes and records data based on the user’s facial characteristics. The device can then be unlocked if the camera detects a face with characteristics that match those of the registered face.

Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Face ID.

d. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

e. As discussed in this affidavit, based on my training and experience I believe that one or more digital devices will be found during the search. The passcode or password that would unlock the device(s) subject to search under this warrant is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the device(s), making the use of biometric features necessary to the execution of the search authorized by this warrant.

f. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be

unlocked using Touch ID when (1) more than 48 hours has elapsed since the device was last unlocked or (2) when the device has not been unlocked using a fingerprint for 4 hours *and* the passcode or password has not been entered in the last 156 hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

g. Due to the foregoing, if law enforcement personnel encounter any device(s) that are subject to seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, the warrant I am applying for would permit law enforcement personnel to obtain from [REDACTED] the display of any physical biometric characteristics (such as fingerprint/thumbprint or facial characteristics) necessary to unlock any device(s), including to (1) press or swipe the fingers (including thumbs) of the aforementioned person to the fingerprint scanner of the device(s); (2) hold the device(s) in front of the face of the aforementioned person to activate the facial recognition feature; and/or (3) hold the device(s) in front of the face of the aforementioned person to activate the iris recognition feature, for the purpose of attempting to unlock the device(s) in order to search the contents as authorized by this warrant.¹³

¹³ The proposed warrant does not authorize law enforcement to require that the aforementioned person to state or otherwise provide the password or identify specific biometric characteristics (including the unique finger(s) or other

CONCLUSION

37. I submit that this affidavit supports probable cause for a warrant to search the PREMISES described in Attachment A and seize the items described in Attachment B.

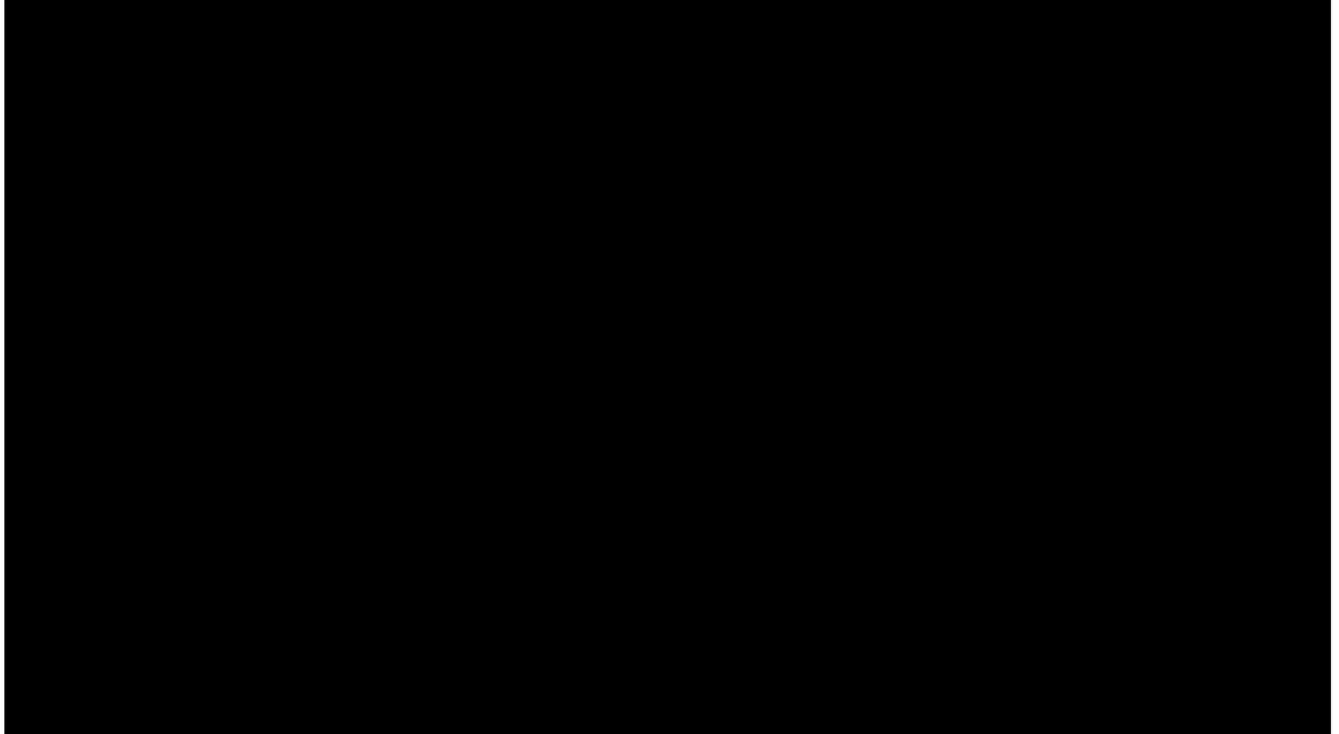
physical features) that may be used to unlock or access the device(s). However, the voluntary disclosure of such information by the aforementioned person(s) would be permitted under the proposed warrant.

ATTACHMENT A

Property to Be Searched

The property to be searched is [REDACTED], CUDAHY, WI 53110, further described as slightly elevated two-story [REDACTED] house with a front porch with a north-facing door and a garage in the back.

google.com/maps/



ATTACHMENT B

Property to Be Seized

1. All records relating to violations of 18 U.S.C. §§ 1028(a)(7) (possession of means of identification in connection with another federal felony offense, including wire fraud); 1029(a)(2) (use and trafficking of access devices), 1029(a)(3) (possession of 15 or more access devices); 1030(a)(2) (illegally accessing a protected computer); 1030(a)(5) (illegally damaging a protected computer); and 371 (conspiracy) (collectively, the “Subject Offenses”) involving [REDACTED] or Web Market A operators and occurring after August 26, 2020, including:

- a. Records and information relating to Web Market A;
- b. Records and information relating to an access, use, possession, or control over stolen personal information, financial information, and/or electronic devices;
- c. Records and information relating to IP address 76.215.26.107;
- d. Records and information relating to the identity or location of the suspect(s);
- e. Records and information relating to malicious software;
- f. Records and information relating to finances, including financial institutions, financial instruments;
- g. Records and information relating to virtual currency such as bitcoin.

2. Computers or storage media used as a means to commit the violations described above.

3. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, “COMPUTER”):

- a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, “chat,” instant messaging logs, photographs, and correspondence;
- b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- c. evidence of the lack of such malicious software;
- d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;
- e. evidence indicating the computer user’s state of mind as it relates to the crime under investigation;
- f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
- g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
- h. evidence of the times the COMPUTER was used;
- i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

- j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
 - k. records of or information about Internet Protocol addresses used by the COMPUTER;
 - l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;
 - m. contextual information necessary to understand the evidence described in this attachment.
4. Routers, modems, and network equipment used to connect computers to the Internet.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term “storage medium” includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

During the execution of the search of the property described in Attachment A, law enforcement personnel are authorized to (1) press or swipe the fingers (including thumbs) of [REDACTED] the fingerprint scanner of the device(s); (2) hold the device(s) in front of the face of [REDACTED] and activate the facial recognition feature; and/or (3) hold the device(s) in front of the face of [REDACTED] and activate the iris recognition feature, for the purpose of attempting to unlock the device(s) in order to search the contents as authorized by this warrant.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.